Available online at www.jmle.org

The National Association for Media Literacy Education's
Journal of Media Literacy Education 8(2), 22 - 34

A Phenomenological Investigation of Social Networking Privacy Awareness through a Media Literacy Lens

David Magolis and Audra Briggs
Bloomsburg University of Pennsylvania

Abstract

This research study focused on the social networking site (SNS) awareness of undergraduate students, examining their experiences through the type and extent of the information shared on their SNSs in order to discover the students' experiences with SNS privacy. A phenomenological research approach was used to interview eight undergraduate to explore the question, "what is the nature of undergraduate students' social networking privacy?" Each recorded interview lasted up to one hour in duration and was transcribed verbatim. A thematic analysis of the interview data revealed that all of the participants were aware of their online privacy, but each had different views about protecting it. The participants that "shared" demographic information on SNSs wanted to be seen and were not worried about their privacy being violated. The participants who were worried about their privacy being violated by someone physically locating them still felt comfortable sharing their personal information. Participants shared at least one type of information about themselves on a SNS but also developed their own settings to protect parts of their privacy.

Keywords: *social networking, privacy, media literacy, phenomenology, undergraduate students*

Since the explosion of social networking sites (SNSs) in the mid 1990's, media users have been increasingly able to create messages in audio, video and multimedia through SNSs. With the increasing use of SNSs in multimedia communication also comes an increased risk of the SNS user's privacy being invaded. A major controversy surrounding SNSs is young adult privacy. Most college students become used to online privacy protection in high school, since 70% of school districts restrict access to SNSs (Lemke et al., 2009). However, when high school students enter college, the restrictions are removed, along with the protection. Understanding, exploring, and preserving undergraduate students' online privacy is a growing concern in media literacy education, and has given rise to a diverse body of research.

Hobbs (1998) emphasizes that media literacy "is a term used by a growing number of scholars and educators to refer to the process of critically analyzing and learning to create one's own messages in print, audio, video, and multimedia" (10) and asks the question, "Should media literacy education aim to protect children and young people from negative media influences?" (18) The influx of SNSs, and the privacy issues surrounding undergraduate students' information sharing on SNSs could be considered a possible cause of negative media influence. According to Potter (2014, 338), "we have reached a point where privacy may be the most important media literacy issue because of the very low level of public awareness about this problem coupled with the risks we all take when we are not aware of these serious threats." Timm and Duven (2008, 90) define SNS privacy as "personal information that an individual deems important and unattainable by the general population." Recently researchers note that there is a high level of privacy awareness among Facebook users (O'Brien and Torres, 2012; Madden and Smith, 2010). But it appears that students are sharing more and more information in SNSs. Rosenblum (2007) reports that social networking users live freely online, while Traddicken (2013) suggests that social media users tend to underestimate the privacy dangers of self-disclosure in SNSs. Potter (2014, 358) notes, "with this issue of privacy, it is essential that you become informed about the risks to your privacy. If you remain ignorant about these risks, you will continue to lose much of your privacy and possibly even your identity."

There has been very little research conducted at the undergraduate level on media literacy, and even less has been conducted on SNSs privacy awareness. Several researchers have studied SNSs and privacy (Lewis, K., Kaufman, J., and Christakis, N., 2008; Hew, 2011; Liu, et. al., 2011), but few have explored privacy awareness in SNSs qualitatively – through undergraduate students' lived experiences. As Schmidt (2013) notes, most of the "existing media literacy research has focused primarily on programs geared towards children and teenagers, especially at the K-12 level…however, much less is known regarding the extent to which media literacy is addressed within postsecondary higher education. What limited research has been done suggests that media literacy may be uncommon on college and university campuses" (296).

Using a media literacy lens, the purpose of this phenomenological study was to explore undergraduates' perceptions of privacy through their lived experiences by seeking answers to the question, "What is the nature of undergraduate students' social networking privacy?" Through a media literacy lens, we can see how the use of SNSs is impacting students' privacy. If we better understand students' perspectives of SNSs privacy through a media literacy lens, we can better design media literacy curricula. What follows is a review of relevant literature that examines media literacy and privacy in SNSs.

Literature Review

Social networking platforms are inherently designed to encourage users to post information (boyd and Ellison, 2007). Waters and Ackerman (2011, 110) explored the research question, "Why do people share personal information on SNSs?" through a survey that identified four motivations for revealing private information on SNSs. The four motivations were to "engage in a fun activity, to store information meaningful to them, to keep up with trends, or to gain popularity." Strater and Lipford (2008) also

studied why information is being shared on SNSs and how it is being protected. They found that the reasons for disclosure of personal information on Facebook were to reinforce relationships with friends and family, to interact with others, and to organize and keep their large social networks up to date.

Govani and Pashley's (2005) study of undergraduates' Facebook profiles shows that an average of 87% of users use the "default" or permissive settings to protect their privacy. The students interviewed in the Strater and Lipford (2008) study said they changed privacy settings only when they first created their profile or after there was a particular incident and also said they did not comprehend how the privacy settings worked because they were too intricate.

These findings, which show the underutilization of privacy controls, raise another common question in the field of study: Are there privacy concerns amongst users? The Gross and Acquisti (2005) study viewed college students' behavior on Facebook to determine if they had privacy concerns or a reason to be concerned. They looked at the different types of information users shared about themselves, such as pictures, friends, and their real name. They named potential privacy threats that could result from the information that is shared. They found that Facebook encourages the use of a user's real name "to connect participants' profiles to their public identities" (Gross and Acquisti, 2005, 72). They also concluded that the degree of friendship is not well shown on Facebook; the information is shared indiscriminately with all of the user's connections, from acquaintances to closest friends. This study shows that the majority of users do not make use of the privacy settings. In the article Gross and Acquisti closed by saying that "personal data is generously provided, [but] limiting privacy preferences are sparingly used" (2005, 79).

In contrast to Gross and Acquisti (2005), Lewis et. al. (2008) found that college students make use of privacy settings; therefore, a concern about their privacy must exist. Lewis, et. al. (2008) attempted to discover what factors are involved when a student chooses between a private or a public profile. They found that students' privacy behavior is influenced by their peers and social life, their high Facebook activity, and by their personal safety reasons. The results showed a third of the students chose to change their default privacy settings, which is a large difference compared to the study by Gross and Acquisti (2005).

Lewis et. al (2008) also noted that students have privacy concerns and Tufekci (2008) researched if this affected the amount of personal information students disclosed. To discover if there was a relationship between personal information exposure and privacy concerns, the Tufecki research question asked how college students managed their audience on Facebook and Myspace while voluntarily sharing information about themselves (Tufekci, 2008). Results showed relatively no relationship between privacy concerns with SNSs and the amount of information shared on SNSs. Instead of limiting the personal information disclosed, students used a false name. On Facebook, they addressed this problem by changing the audience visibility settings. Again, the norm of using a real name on Facebook was seen. This study, along with several others, showed choices were being made about privacy settings, but few of these studies examined privacy awareness from the users' perspective. Therefore, we asked the question: What is the nature of undergraduate students' social networking privacy? What follows is a study

that explores undergraduate students' privacy awareness in SNSs, by seeking answers to the following questions:

1. What information do undergraduate students share on SNSs?
2. Why do undergraduate students share personal information on SNSs?
3. How do undergraduate students describe their use of social networking privacy?
4. How are undergraduate students managing their personal information exposure in SNSs?

Methods

Research related to undergraduate students' online privacy, SNSs, and their sharing of personal information has made great strides in the past few years. However, there is very little that explores online privacy from students' own vantage points. A phenomenological research method provides first-hand insight into the decisions students make involving their online privacy on SNSs. "Phenomenology does not produce empirical or theoretical observations or accounts. Instead, it offers accounts of experienced space, time, body, and human relations as we live them" (Van Manen, 1990, 184).

Participants. Eight undergraduate students at a northeastern United States university participated in this study. All participants were seniors with different bachelor degree concentrations. Participants included four males and four females ages 20 to 22. Table 1 shows a chart with descriptions of each participant, their pseudonym, and their social media usage.

Procedure. Each participant was interviewed face-to-face by the researchers. All interview questions were open-ended, except for a few demographic questions. The open-ended questions permitted the researchers to obtain rich descriptions of the participants' lived experiences. Participants were interviewed twice during the Semester. The interviews lasted 60 and 30 minutes, respectively. The interviews were audio-recorded and transcribed verbatim. Once transcribed, the interviews were analyzed for similarities and recurring themes among the participants' answers.

Data Analysis. The data was analyzed following the phenomenological approach (Dahlberg et. al. 2008). Two researchers individually read the whole data set, which included all transcripts and field notes, along with memos generated from the interviews. After acquiring a firm comprehension of the entire data set, the researchers read each interview and brief memos were generated for the individual interviews. The interviews were read a third time before the interviews were coded line-by-line. Line-by-line coding generated meaning units from the participants' statements concerning the phenomenon. Those meaning units were then discussed and analyzed by the researchers during four separate periods to identify common themes. A total of nine meaning units were identified and clustered (based upon similarities) into general themes. The researchers continued to analyze the transcripts, memos and field notes until no more themes were discovered and the data reached a point of saturation (i.e. no new additional insights were generated).

Table 1
Participant Profiles

	Females				Males			
	Kristina	Lena	Morgan	Liz	Mike	Mark	Dom	John
Age	21	22	21	22	22	20	22	22
Race	*CAU	Filipino	CAU	CAU	CAU	CAU	CAU	CAU
Work	Part time	N/A	Part time	Full time	Part time	Part time	N/A	Part time
Social Media	Twitter, public; **FB, Private; Instagram, public; Tumblr, public	Twitter, public; Instagram, public; Linked In, public; YouTube, public; Pinterest, public; Google Plus, public	Twitter, private; FB, private; Instagram, public; LinkedIn, public	Twitter, public; FB, private only friends of friends can view profile; LinkedIn, public; Pinterest, public; Google Plus, public; College Central, public; Monster, public; Fastweb, public	Twitter, public; FB, Public; YouTube, Public; Reddit, public	Twitter, public; FB, private; Instagram, private; LinkedIn, private; YouTube, public; Vimeo, public	Twitter, public; FB, public; information, private statuses; Instagram, public	Twitter, public; FB, public
How often do you log onto your social networking site?	Never logs out	Logs on every day to Instagram Twitter, Linked In, and Pinterest	Checks all daily	Checks FB everyday	Reddit and FB multiple times a day	Daily on Twitter, FB	All media throughout the day	FB 1 or 2 times a day; Twitter 10 to 15 times a day
How often do you update a status?	Tumblr constantly; FB 1 or 2 times a month; Twitter several times a month	Twitter multiple times a day. Instagram twice a day or once a couple days.	Instagram once or twice a day	No response	4 or 5 times a month	0-2 on FB a day 20-50 times on Twitter	10 times a day on FB	1 time a week on FB; 0-3 times a day for twitter
How many friends do you have?	Tumblr 90; Twitter 60; FB 100	Instagram 200	Twitter 430; FB over 2000; Instagram 400	FB 500; Google + 20	FB 580	FB 1300; Twitter 283; Instagram 128	FB 400; Twitter 100; Instagram 100	FB 800; Twitter 67

*CAU is Caucasian, **FB is Facebook

Findings

For the purpose of this study, the two types of shared information that participants talked about were categorized into personal and background information. Throughout this paper, the term "personal information" refers to a person's interests, likes, dislikes, and any other non-demographic facts. The term "background information" refers to any demographic means of locating or identifying a person--such as age, hometown, sex, etc. Participants also differentiated between private and public profiles. A "public profile" is defined as those which anyone online can view. A "private profile" is defined as one where the owner sets perimeters for viewers.

All participants had at least one SNS. These sites included Facebook (FB), Twitter, Instagram, Tumblr, Reddit, Youtube, LinkedIn, Pinterest, Google Plus, Vimeo, and other sites. Only one participant did not have a FB account, which was a shared theme among the rest. All participants logged onto at least one of their SNSs daily. Participants were aware they could withdraw from the study at any time, and received no incentive such as extra credit or monetary awards. What follows are the results from the interviews. The exhaustive themes are displayed in the sections below.

Theme 1: Openly Shared Personal Information

To explore the first guided research question, participants were asked, "What do you share on your social networking sites?" All eight participants had at least one public profile; five participants shared personal information with the public on at least one of their SNSs. The participants shared information that would not specifically locate or identify them, but would enable others to emotionally connect to them – music and movie interests, "Likes", Recent Activity, etc. The three major SNSs in which personal information was shared were Facebook, Pinterest, and Tumblr. Facebook's "About Me" and "Favorites" sections, Pinterest's boards, and Tumblr's blogs were all methods utilized by the participants to share information about their interests.

Ease of sharing personal information. O'Brien and Torres' (2012) research of active Facebook users found that half of the participants had a high level of privacy awareness on Facebook. If students have high privacy awareness, what are students' experiences with sharing information in SNSs? Five participants--Mike, Lena, Liz, Dom, and John--shared their personal information on a public SNS profile. When asked, "What do you share on your social networking sites?" Mike described the content of his publicly available profile as "very detailed." He continued to explain that he started a Facebook profile at age sixteen, and since then has added to the About Me and Favorites sections resulting in his profile being "very extensive." He continued, "I guess as far as [personal] information, people can know whatever, almost anything they want about me from my Facebook."

Dom also recognized how Facebook made getting to know someone easier through their information in the About Me and Favorite sections. He stated, "When you know someone in person, you have to specifically ask them what kind of movies do you like? What kind of music do you like? All that kind of stuff versus just being friends with someone on Facebook, all that stuff's available at a finger click." Facebook, along with other SNSs, do a masterful job of enabling users to easily share personal information. When users allow the public to view their personal information, personal privacy is easily

compromised. Simply sharing information including Likes, Comments, and song lyrics provides viewers with a character profile.

Kristina, who does not share her name on Tumblr, explains how a stranger could develop a character sketch of her by what she shared on the SNS Tumblr:

> I mean, obviously if somebody cared to do a character study of me, they would find a lot more information about myself as a person based on what I post on Tumblr just because if you really were that deep about it, you could look at what my favorite scenes are, what the stuff is that speaks to me the most from this band, and what are the lyrics that I really like, that I always talk about.

These five participants were aware that their profiles were viewable to everyone, and were comfortable sharing their interests, likes, opinions, and other non-demographic facts. The personal facts that are usually learned when developing a personal friendship are now easily broadcast to viewers on SNSs. By sharing extensive personal information, users are giving any public viewer the opportunity to be their "friend" and compromising their privacy. We found that the information users share on SNSs is detailed, and that most participants of this study are comfortable sharing their personal information.

Subtheme - Don't Cross the Line: Limits on Personal Location

In the interviews, one subtheme that emerged was participants' unwillingness to share their physical locations on SNSs. Kristina explained that she shared information on Tumblr that revealed her personality and character. However, she limited information on her physical location because "my online privacy, I think, is more me worried about physically being able to be located." Kristina worried about a stranger locating her, so she did not share her name, address, and other background information that could lead to some type of physical danger. But she acknowledges how other information posted to SNSs can determine your location. She concluded:

> I feel like on Facebook, you like a bunch of restaurants that are in your area, even if you don't have your town [listed in public profile] people will still know where you live…I'm worried about my online privacy in the respect of physically locating where I am rather than knowing information about me as a person… So I don't care if people know that I'm obsessed with Harry Potter, but I don't want them to know the street that I live on or my phone number to contact me.

This quote demonstrates that Kristina is knowledgeable about how someone could use her information, and chooses to share no information that could hint to her location. Liz had similar views of openly sharing personal information. She said:

> I have no problem with people knowing what I like. If they connect with me over that, sure, whatever, that's cool. Finding people that you don't know face to face, but you can actually relate to is nifty. Just as long as you don't cross that line, and you're not going to say "Hey, meet me in a dark alley in New York." That's crossing the line a little bit.

Like Liz, the other participants explained how they connected to others online through similar likes and interests and how they enjoyed this type of networking. However, even though they shared interests with their online friends, Mark, Morgan and Kristina did not want to know the people in their virtual community in real life. They also clearly identified the difference between sharing background and personal information, with background information being described as facts that could allow them to be located offline, in real life. They see connecting with people online as being safe, as long the line is not crossed. According to our participants, this line is drawn when meeting the virtual friend in person or under suspicious circumstances.

The participants do not consider a stranger knowing about their personality as a privacy violation, but do consider a stranger's knowledge of their physical location to be an extreme violation of privacy. Participants were comfortable sharing their non-demographics with the public. They were also comfortable with connecting to others online that had the same interests. However, to the participants, being located by someone they connected to online constituted online privacy violation.

Theme 2: I Want to be Seen

John, Mike, Lena, and Dom all expressed a desire to be "seen," stating that they openly shared their demographics to the public on SNSs because they want to be contacted. Self-described as familiar with privacy settings, they made the decision to have a public profile, thus allowing the public to view their background information and intimate personal details such as their first and last names, birthday, email address, schools attend, and cellphone number. When asked the question, "Why don't you feel the need to keep personal information private?" Dom responded on "Facebook I share pretty much everything. I even have my phone number and email address on there." Collectively, participants stated that sharing "pretty much everything" makes it easier for non-friends to access and communicate with them online. In fact, these participants wanted to provide others with an easy means to connect with them online. Mike said, "Ever since I made [my profile], I knew it was public. I like sharing my views with the public and getting their input."

Subtheme - Choosing what to share could lead to employment. Much of the discussion for this subtheme was the advantages of SNSs for employment opportunities. One of the main responses to the question, "why don't you feel the need to keep personal information private" was to assist the users in developing their career. John explains, "I know everyone looks at Facebook and Twitter at this point, so I want them to be able to find me." Participants agreed that using a public SNS profile could lead to professional networking. Mike, Dom, and John wanted professionals in their field to have an easy method to contact them. John stated:

> My Twitter and everything is all out there to make it easy for potential employers to contact me, to find me.…If a potential employer were to look for my Facebook and/or Twitter, I would want them to be able to find it easily and see what's on it. I just make sure that everything on it could be seen in a positive light.

Mike further illustrated his attempt to network with professionals by stating, "I find myself friending, I guess, more acquaintances than actual friends…I've got people

on my friends list that are professionals in the field and people that I've talked to in the past that might have internship ideas for me." Mike and John considered it possible to increase their social capital by allowing more acquaintances to be their "friend" online. By friending unfamiliar individuals and subsequently allowing their background information to be easily viewed, Mike is trying to increase his chance of having a better career. Mike even sought to make it easy as possible for a potential employer to find him, "So if they want to find me on Twitter, I want it to be as easy as possible. I don't want them to have to remember some weird, odd, Twitter handle."

Mike, Dom, and John hope to use their SNS accounts to win job offers from potential employers. Therefore, the users are cautious about sharing certain information, but are unrestricted in displaying personal background information on SNSs if they feel that the information can improve their chances of employment. Mike, Dom and John anticipated future employers viewing their profiles, and consciously constructed those profiles to establish a good online presence that would interest potential employers.

Subtheme - Online Danger. Online crimes such as fraud, phishing, and identity theft have been well documented in the research literature (MacEwan, 2013; Wall, 2010; Choo, 2011). As previously noted, participants expressed various levels of comfort with the information they shared on their public SNS profiles, including personal background information. Some went so far as to mention that there is no danger in sharing intimate details online. We asked the question, "Why don't you feel the need to keep personal information private?" During a conversation about the content of his background information, Mike said:

> I give people the benefit of the doubt a very large majority of the time. I'm not the type of person that's thinking people are going to take advantage of that information… I think I might have been hacked on my Facebook once. And even when that happened, I knew how to change my password, so it was not a big deal.

Dom agreed, stating, "I've never gotten any death threats texted to me. I don't ever worry that someone's going to track me down from my Facebook and do something to me." This quote indicates a trust of SNSs as safe public venues. However, crimes such as identity thefts have occurred on SNSs. In spite of this fact, the thought that a predator would target their profiles and try to harm them was not a realistic fear for the participants. Mark said, "If someone wants to contact me, even if they're a stranger, they can contact me. If it's my cell phone, they can leave a message. If they're creepy, I never have to call them back." These participants do not feel threatened by a stranger's online contact, although such contact could lead to an online privacy violation.

Theme 3: Personalized Privacy Settings

The participants described themselves as belonging to one of two factions when it came to privacy settings: participants with private profiles and those with public profiles. Participants with private profiles made use of the available privacy settings and both types of participants took additional steps to develop their own privacy settings. Both private and public profile users had a sense of control over their SNSs. As explained throughout the interviews, participants made specific decisions regarding what information they share. We asked the question, "How would you describe your use of

SNSs' privacy settings?" Every participant interviewed explained how he or she developed some type of privacy setting.

Subtheme - Self-censoring. All participants described a time when they censored a picture or post they thought was a sensitive topic. Dom said, "I'm more reserved online. I – I censor myself a little bit just to – because I don't want to – I don't feel like offending people on there." This shows that Dom makes specific decisions on keeping some of his opinions private so as not to offend anyone. According to the participants, the most censored topics were politics and religion. Participants strongly agreed that political opinions should be censored and not shared at all. Kristina strongly opposed posting political or religious exchanges on SNSs by expressing, "I don't post political things. I don't post controversial stuff. I don't like when people talk about religion or, you know, politics." Similarly, Liz also avoided political conversations, "I try and stay away from things, especially if I'm, like, annoyed about something, I don't voice, say, my political opinion… I am very, very, um, careful about what I put on." John agreed that keeping comments politically correct on SNSs was important, stating, "I never post about politics or anything like that on Facebook. You know, try to keep it PC [politically correct]."

Participants also self-censored themselves on SNSs by withholding of certain pieces of information. Kristina said, "My name's not on my Tumblr, and I don't have my pictures on it." She continues on Facebook, "I don't have my school listed... I don't have my phone number up there, and a lot of people have that... My birthday is on there but not where I live." Four other participants similarly withheld information by sharing only certain parts of their background information on SNSs. For example, Mike said, "My cell phone is on there but, without the area code." Three participants stated that they share their birthday, but not the year they were born. Even when Facebook has the option and space for users to post their phone number, birthday, and location, participants largely ignored those demographic options, withholding the information to protect their privacy.

All of the participants created their own privacy settings by making specific decisions on what to share and not to share. Two participants used a nickname instead of their whole name to remain anonymous, or to make it difficult for people to find them. They all believe they have a good sense of what is right and wrong to put up on their profile. They determined what was appropriate by using their own judgment; some also considered how their audience would react before posting. These findings show that undergraduate students are aware of their online privacy and they are making their own decisions to protect it, not by using the privacy settings available, but through various methods they developed. They are taking the initiative to keep certain aspects of their lives private, echoing the findings of Lewis, et. al. (2008) who found that concern about privacy must exist among college students because they are using the privacy settings. Our findings show, however, that the participants in this study created their own privacy settings instead of using the ones already available.

Conclusion

This study explored the phenomenon of undergraduate students' privacy awareness on SNS, finding that students were aware of their online privacy but had different views about protecting it. Some took actions to protect their information, while others were comfortable being completely open on SNSs.

During this transition from high school to college to professional life, profile creators need media literacy education to help discern what information is acceptable on SNSs. This should not be a one-time class, but an on-going educational experience. Online privacy is constantly changing as easier-to-use technologies are developed to share personal information. Overall, every participant either shared personal or background information with the public. Those who shared a large amount of information, especially background information, wanted to be seen and contacted.

The participants associated having an open SNS profile with networking, career enhancement, and job opportunities. Do open SNS profiles actually lead to any of these goals sought by our participants? Future research should explore the potential of open SNS profile and job obtainment. Furthermore, do potential employers desire all of the personal information in SNS before hiring a candidate? Should employers require that certain information be shared online to help with the hiring process?

Perhaps a course designed to establish SNS parameters for employee/employer relationships would improve overall media literacy at the undergraduate level. Potter (2013, 422) explains, "No one is born media literate. Media literacy must be developed, and this development requires effort from each individual as well as guidance from experts. The development also is a long-term process that never ends, that is, no one ever reaches a point of total, complete media literacy." Therefore, media literacy educators might consider developing a curriculum based on media literacy and employee/employer relationships on SNSs at various educational levels, including the post-graduate adult level.

Participants who were worried about their online privacy being violated by someone physically locating them still felt comfortable sharing their personal information. They did not mind if someone connected to them through their similar interests. Six out of the eight participants stated that they shared very detailed personal information about themselves on their public profiles. This shows that while some were worried about being located, most were comfortable sharing their interests, likes, and non-demographic facts. We concur with the research by Vanderhoven, Schellens and Valcke (2013) that raising the awareness and the care about SNS privacy with young adults might be helpful, and that universities are ideal places for fostering such awareness.

Results indicated that participants also created their own privacy settings. These settings included withholding information by not sharing it online, using a nickname, or having two separate profiles for personal and professional roles. Results show that participants are aware of their SNS privacy, because they were making cognizant decisions to protect themselves. However, what is the optimal privacy setting? We suggest that high school and undergraduate education initiatives should strive to prepare students for careful participation in SNSs. Research studies that are focused on SNS privacy should remember that these sites are constantly changing, and that personal privacy settings are changing with them. Future research will always bring new perspectives due to the constantly changing SNSs. The current generation of undergraduate students grew up with Myspace, moved on to Facebook, and now utilize Twitter on a daily basis. Future studies should focus on undergraduate students who are immersed in the world of SNSs by examining undergraduate students who have and have not received media literacy training or instruction--and their privacy awareness. In this

study, we used the phenomenological method to understand undergraduate students' privacy in SNS through their lived experiences. Results from this report can assist (a) researchers, in their drive to understand undergraduate students' SNS privacy, (b) institutions, in responding to media literacy curriculum changes, (c) higher education career development centers working with students to develop their media literacy for job searching, and (d) individual faculty who teach emerging technologies and how they relate to undergraduate students. More research is needed to examine undergraduate students' SNS privacy and educational programs that address SNS privacy. By taking such steps to improve undergraduate students' media literacy, the study will possibly help develop the individual's understanding of the dynamic nature of SNS online privacy.

References

boyd, D. M., and N. B. Ellison. 2007. Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication* 13 (1): 210-30.

Choo, Kim-Kwang Raymond. 2011. The cyber threat landscape: Challenges and future research directions. *Computers & Security* 30 (8): 719-31.

Dahlberg, Karin. 2008. *Reflective lifeworld research*. Lund: Studentlitteratur.

Govani, Tabreez, and Harriet Pashley. 2005. Student awareness of the privacy implications when using Facebook. *Unpublished Paper Presented at the "Privacy Poster Fair" at the Carnegie Mellon University School of Library and Information Science* 9.

Gross, Ralph, and Alessandro Acquisti. 2005. Information revelation and privacy in online social networks. Paper presented at Proceedings of the 2005 ACM workshop on Privacy in the electronic society, Proceedings of the 2005 ACM workshop on Privacy in the electronic society.

Hew, K. F. 2011. Students' and teachers' use of Facebook. *Computers in Human Behavior* 27 (2): 662-76.

Hobbs, R. 1998. The seven great debates in the media literacy movement. *Journal of Communication, 48 (2)*, 9-29.

Lemke, Cheryl, Ed Coughlin, Lauren Garcia, Daren Reifsneider, and Jessica Baas. 2009. Leadership for web 2.0 in education: Promise and reality. Culver City, CA.

Lewis, K., J. Kaufman, and N. Christakis. 2008. The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication* 14 (1): 79-100.

Liu, Yabing, Krishna P. Gummadi, Balachander Krishnamurthy, and Alan Mislove. 2011. Analyzing Facebook privacy settings: User expectations vs. reality. Paper presented at Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference.

MacEwan, Neil. 2013. A tricky situation: Deception in cyberspace. *Journal of Criminal Law* 77 (5): 417-32.

Madden, Mary K., and Aaron Whitman Smith. 2010. *Reputation management and social media: How people monitor their identity and search for others online.* Washington D.C.: Pew Internet & American Life Project, http://www.pewinternet.org/2010/05/26/reputation-management-and-social-media/.

O' Brien, Deirdre, and Ann M. Torres. 2012. Social networking and online privacy: Facebook users' perceptions. *Irish Journal of Management* 31 (2): 63-97.

Phillips, Kristen. 2012. *Identifying media consumption habits and media literacy skills in college undergraduates*. Master of Arts., University of Texas at Arlington, http://dspace.uta.edu/handle/10106/11128?show=full.

Potter, W. J. 2014. *Media literacy*. 7th ed. Los Angeles: CA: Sage.

———. 2013. *Media literacy*. 6th ed. Los Angeles: CA: Sage.

Rosenblum, David. 2007. What anyone can know: The privacy risks of social networking sites. *IEEE Security and Privacy* 5 (3): 40-49.

Schmidt, Hans C. 2013. Media literacy education from kindergarten to college: A comparison of how media literacy is addressed across the educational system. *Journal of Media Literacy Education* 5 (1): 295-309.

Strater, Katherine, and Heather Richter Lipford. 2008. Strategies and struggles with privacy in an online social networking community. Paper presented at Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction-Volume 1.

Timm, Dianne M., and Carolyn J. Duven. 2008. Privacy and social networking sites. *New Directions for Student Services* (124): 89-101.

Tufekci, Zeynep. 2008. Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society* 28 (1): 20-36.

Van Manen, Max. 1990. *Researching lived experience: Human science for an action sensitive pedagogy*. Albany, NY: State University of New York Press.

Vanderhoven, Ellen, Tammy Schellens, and Martin Valcke. 2013. Exploring the usefulness of school education about risks on social network sites: A survey study. *Journal of Media Literacy Education* 5 (1): 285-94.

Wall, David. 2010. The internet as a conduit for criminal activity. In *Information technology and the criminal justice system.* Ed. Pattavina, A. 77-98. Thousand Oaks: CA: Sage.

Waters, Susan, and James Ackerman. 2011. Exploring privacy management on Facebook: Motivations and perceived consequences of voluntary disclosure. *Journal of Computer-Mediated Communication* 17 (1): 101-15.